Malware and Viruses 101

One common mistake that people make when the topic of a computer virus arises is to refer to a worm or Trojan horse as a virus. While the words Trojan, worm and virus are often used interchangeably, they are not exactly the same thing. Viruses, worms and Trojan Horses are all malicious programs that can cause damage to your computer, but there are differences among the three, and knowing those differences can help you better protect your computer from their often damaging effects.

What Is a Virus?

A computer virus attaches itself to a program or file enabling it to spread from one computer to another, leaving infections as it travels. Like a human virus, a computer virus can range in severity: some may cause only mildly annoying effects while others can damage your hardware, software or files. Almost all viruses are attached to an executable file, which means the virus may exist on your computer but it actually cannot infect your computer unless you run or open the malicious program. It is important to note that a virus cannot be spread without a human action, (such as running an infected program) to keep it going. Because a virus is spread by human action people will unknowingly continue the spread of a computer virus by sharing infecting files or sending emails with viruses as attachments in the email.

What Is a Worm?

A worm is similar to a virus by design and is considered to be a sub-class of a virus. Worms spread from computer to computer, but unlike a virus, it has the capability to travel without any human action. A worm takes advantage of file or information transport features on your system, which is what allows it to travel unaided.

The biggest danger with a worm is its capability to replicate itself on your system, so rather than your computer sending out a single worm, it could send out hundreds or thousands of copies of itself, creating a huge devastating effect. One example would be for a worm to send a copy of itself to everyone listed in your e-mail address book. Then, the worm replicates and sends itself out to everyone listed in each of the receiver's address book, and the manifest continues on down the line.

Due to the copying nature of a worm and its capability to travel across networks the end result in most cases is that the worm consumes too much system memory (or network bandwidth), causing Web servers, network servers and individual computers to stop responding. In recent worm attacks such as the much-talked-about Blaster Worm, the worm has been designed to tunnel into your system and allow malicious users to control your computer remotely.

What Is a Trojan horse?

A Trojan Horse is full of as much trickery as the mythological Trojan Horse it was named after. The Trojan Horse, at first glance will appear to be useful software but will actually do damage once installed or run on your computer. Those on the receiving end of a Trojan Horse are usually tricked into opening them because they appear to be receiving legitimate software or files from a legitimate source. When a Trojan is activated on your computer, the results can vary. Some Trojans are designed to be more annoying than malicious (like changing your desktop, adding silly active desktop icons) or they can cause serious damage by deleting files and destroying information on your system. Trojans are also known to create a backdoor on your computer that gives malicious users access to your system, possibly allowing confidential or personal information to be compromised. Unlike viruses and worms, Trojans do not reproduce by infecting other files nor do they self-replicate.

What Are Blended Threats?

Added into the mix, we also have what is called a blended threat. A blended threat is a more sophisticated attack that bundles some of the worst aspects of viruses, worms, Trojan horses and malicious code into one single threat. Blended threats can use server and Internet vulnerabilities to initiate, then transmit and also spread an attack. Characteristics of blended threats are that they cause harm to the infected system or network, they propagates using multiple methods, the attack can come from multiple points, and blended threats also exploit vulnerabilities.

To be considered a blended thread, the attack would normally serve to transport multiple attacks in one payload. For example it wouldn't just launch a DoS attack — it would also, for example, install a backdoor and maybe even damage a local system in one shot. Additionally, blended threats are designed to use multiple modes of transport. So, while a worm may travel and spread through e-mail, a single blended threat could use multiple routes including e-mail, IRC and file-sharing sharing networks.

Lastly, rather than a specific attack on predetermined .exe files, a blended thread could do multiple malicious acts, like modify your exe files, HTML files and registry keys at the same time — basically it can cause damage within several areas of your network at one time.

Blended threats are considered to be the worst risk to security since the inception of viruses, as most blended threats also require no human intervention to propagate.

Tips to Combat Viruses, Worms and Trojan Horses on Your Computer

Keep the Operating System Updated

The first step in protecting your computer from any malicious there is to ensure that your operating system (OS) is up-to-date. This is essential if you are running a Microsoft Windows OS. Secondly, you need to have anti-virus software installed on your system and ensure you download updates frequently to ensure your software has the latest fixes for new viruses, worms, and Trojan horses. Additionally, you want to make sure your anti-virus program has the capability to scan e-mail and files as they are downloaded from the Internet, and you also need to run full disk scans periodically. This will help prevent malicious programs from even reaching your computer.

Use a Firewall

You should also install a firewall. A firewall is a system that prevents unauthorized use and access to your computer. A firewall can be either hardware or software. Hardware firewalls provide a strong degree of protection from most forms of attack coming from the outside world and can be purchased as a stand-alone product or in broadband routers. Unfortunately, when battling viruses, worms and Trojans, a hardware firewall may be less effective than a software firewall, as it could possibly ignore embedded worms in outgoing e-mails and see this as regular network traffic.

For individual home users, the most popular firewall choice is a software firewall. A good software firewall will protect your computer from outside attempts to control or gain access your computer, and usually provides additional protection against the most common Trojan programs or e-mail worms. The downside to software firewalls is that they will only protect the computer they are installed on, not a network.

It is important to remember that on its own a firewall is not going to rid you of your computer virus problems, but when used in conjunction with regular operating system updates and a good anti-virus scanning software, it will add some extra security and protection for your computer or network.